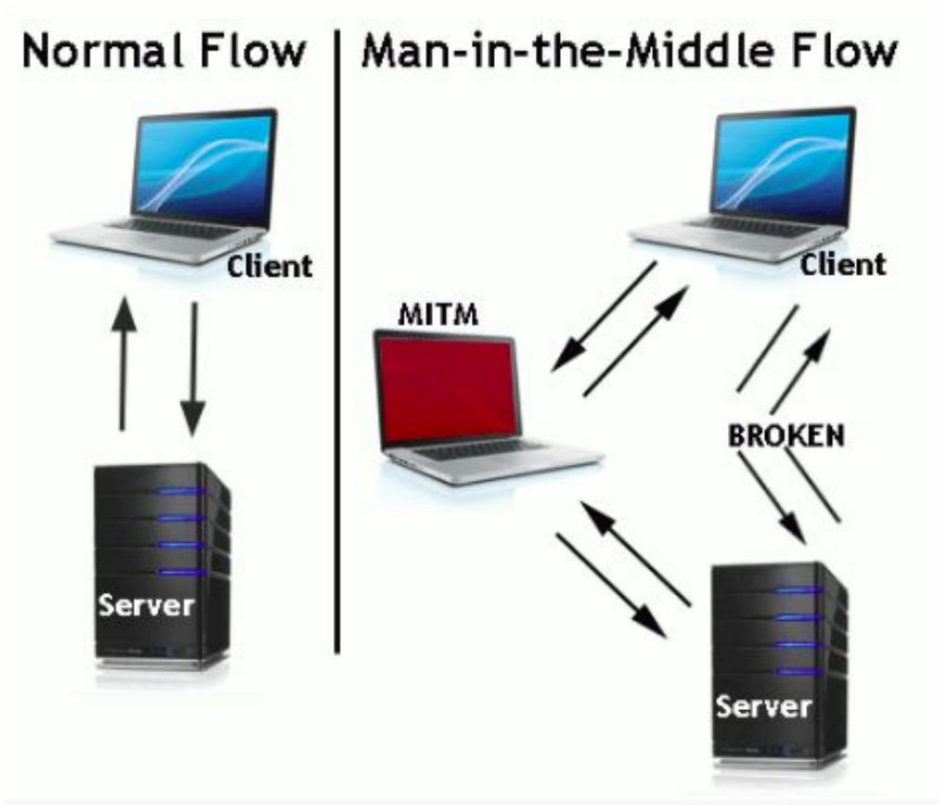
MAN IN THE MIDDLE (MITM) ATAQUE

Um ataque man-in-the-middle é um tipo de ataque cibernético em que um ator mal-intencionado se insere em uma conversa entre duas partes, se faz passar por ambas as partes e obtém acesso às informações que as duas partes estavam tentando enviar uma à outra. Um ataque man-in-the-middle permite que um ator mal-intencionado intercepte, envie e receba dados destinados a outra pessoa, ou não destinados a serem enviados, sem que nenhuma das partes externas saiba até que seja tarde demais. Os ataques man-in-the-middle podem ser abreviados de várias maneiras, incluindo MITM, MitM, MiM ou MIM.

Conceitos-chave de um ataque man-in-the-middle

- **ÿ Man-in-the-middle é um tipo de ataque de espionagem que ocorre quando um ator malicioso se insere como um retransmissor/proxy em uma sessão de comunicação entre pessoas ou sistemas.**
- **ÿ Um ataque MITM explora o processamento em tempo real de transações, conversas ou transferência de outros dados. ÿ**
- **Os ataques man-in-the-middle permitem que os invasores interceptem, enviem e recebam dados que nunca deveriam ser para eles sem nenhum dos dois parte externa sabendo até que seja tarde demais.**

Exemplos de ataque man-in-the-middle



Tipos de ataques man-in-the-middle

Ponto de acesso não autorizado

Os dispositivos equipados com placas sem fio geralmente tentam se conectar automaticamente ao ponto de acesso que está emitindo o sinal mais forte. Os invasores podem configurar seu próprio ponto de acesso sem fio e enganar os dispositivos próximos para ingressar em seu domínio. Todo o tráfego de rede da vítima agora pode ser manipulado pelo invasor. Isso é perigoso porque o invasor nem precisa estar em uma rede confiável para fazer isso — o invasor simplesmente precisa de uma proximidade física suficiente.

Falsificação de ARP

ARP é o Protocolo de Resolução de Endereço. Ele é usado para resolver endereços IP para endereços físicos MAC (controle de acesso à mídia) em uma rede local. Quando um host precisa falar com um host com um determinado endereço IP, ele faz referência ao cache ARP para resolver o endereço IP para um endereço MAC. Se o endereço não for conhecido, é feita uma solicitação solicitando o endereço MAC do dispositivo com o endereço IP.

Um invasor que deseja se passar por outro host pode responder a solicitações às quais não deveria estar respondendo com seu próprio endereço MAC. Com alguns pacotes colocados com precisão, um invasor pode farejar o tráfego privado entre dois hosts. Informações valiosas podem ser extraídas do tráfego, como troca de tokens de sessão, fornecendo acesso total a contas de aplicativos que o invasor não deveria ter acesso.

Falsificação de mDNS

O DNS multicast é semelhante ao DNS, mas é feito em uma rede local (LAN) usando transmissão como ARP. Isso o torna um alvo perfeito para ataques de falsificação. O sistema de resolução de nomes locais deve tornar a configuração dos dispositivos de rede extremamente simples. Os usuários não precisam saber exatamente com quais endereços seus dispositivos devem se comunicar; eles deixam o sistema resolver isso para eles. Dispositivos como TVs, impressoras e sistemas de entretenimento usam esse protocolo, pois geralmente estão em redes confiáveis. Quando um aplicativo precisa saber o endereço de um determinado dispositivo, como tv.local, um invasor pode facilmente responder a essa solicitação com dados falsos, instruindo-o a resolver para um endereço sobre o qual tem controle. Como os dispositivos mantêm um cache local de endereços, a vítima agora verá o dispositivo do invasor como confiável por um período de tempo.

Falsificação de DNS

Semelhante à maneira como o ARP resolve endereços IP para endereços MAC em uma LAN, o DNS resolve nomes de domínio para endereços IP. Ao usar um ataque de falsificação de DNS, o invasor tenta introduzir informações de cache DNS corrompidas em um host na tentativa de acessar outro host usando seu nome de domínio, como www.onlinebanking.com. Isso leva a vítima a enviar informações confidenciais a um host mal-intencionado, acreditando que está enviando informações a uma fonte confiável. Um invasor que já falsificou um endereço IP pode ter muito mais facilidade em falsificar o DNS simplesmente resolvendo o endereço de um servidor DNS para o endereço do invasor.

Técnicas de ataque man-in-the-middle

cheirar

Os invasores usam ferramentas de captura de pacotes para inspecionar pacotes em um nível baixo. O uso de dispositivos sem fio específicos que podem ser colocados em modo de monitoramento ou promíscuo pode permitir que um invasor veja pacotes que não devem ser vistos, como pacotes endereçados a outros hosts.

Injeção de pacote

Um invasor também pode aproveitar o modo de monitoramento de seu dispositivo para injetar pacotes maliciosos em fluxos de comunicação de dados. Os pacotes podem se misturar com fluxos de comunicação de dados válidos, parecendo fazer parte da comunicação, mas de natureza maliciosa. A injeção de pacotes geralmente envolve primeiro sniffing para determinar como e quando criar e enviar pacotes.

Sequestro de Sessão

A maioria dos aplicativos da Web usa um mecanismo de login que gera um token de sessão temporário para usar em solicitações futuras para evitar que o usuário digite uma senha em todas as páginas. Um invasor pode farejar tráfego confidencial para identificar o token de sessão de um usuário e usá-lo para fazer solicitações como o usuário. O invasor não precisa falsificar uma vez que tenha um token de sessão.

Decapagem de SSL

Como o uso de HTTPS é uma proteção comum contra a falsificação de ARP ou DNS, os invasores usam a remoção de SSL para interceptar pacotes e alterar suas solicitações de endereço baseadas em HTTPS para ir para o endpoint equivalente a HTTP, forçando o host a fazer solicitações ao servidor não criptografadas. Informações confidenciais podem vazar em texto simples.

Prevenção de ataques man-in-the-middle

Criptografia WEP/WAP forte em pontos de acesso

Ter um forte mecanismo de criptografia em pontos de acesso sem fio impede que usuários indesejados entrem na sua rede apenas por estarem próximos. Um mecanismo de criptografia fraco pode permitir que um invasor entre em uma rede com força bruta e comece a atacar man-in-the-middle. Quanto mais forte a implementação da criptografia, mais segura.

Rede Privada Virtual

As VPNs podem ser usadas para criar um ambiente seguro para informações confidenciais em uma rede local. Eles usam criptografia baseada em chave para criar uma sub-rede para comunicação segura. Dessa forma, mesmo que um invasor entre em uma rede compartilhada, ele não conseguirá decifrar o tráfego na VPN.

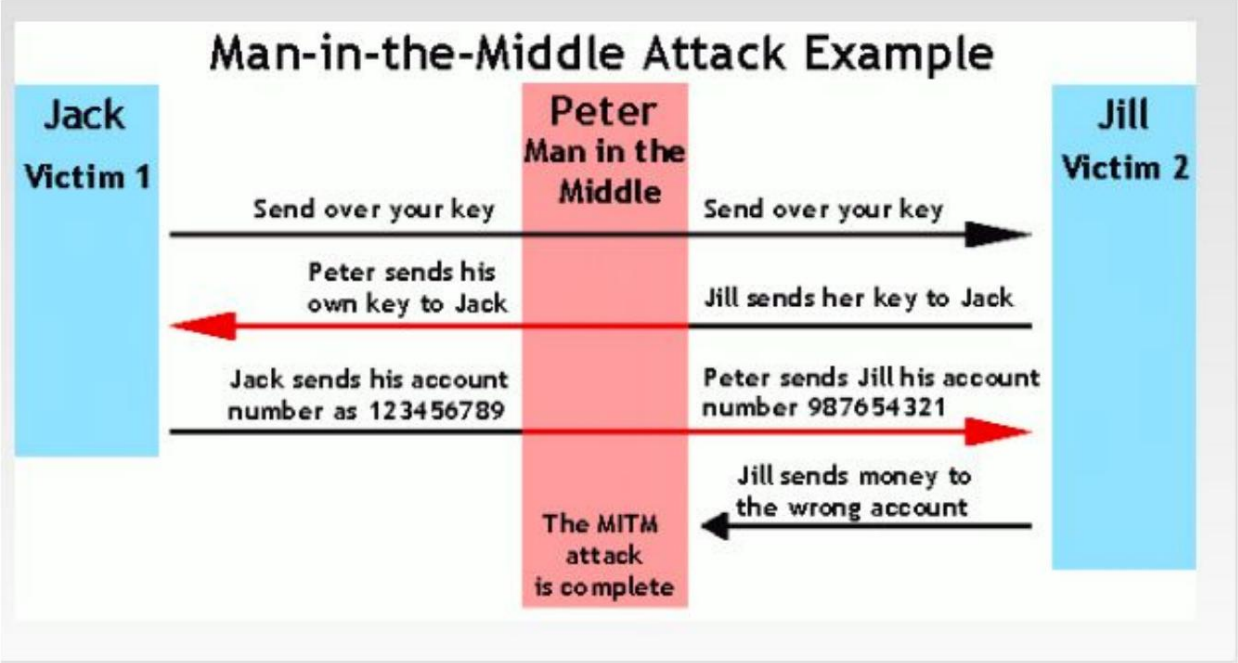
Forçar HTTPS

O HTTPS pode ser usado para se comunicar com segurança por HTTP usando a troca de chaves público-privadas. Isso evita que um invasor tenha qualquer uso dos dados que ele pode estar farejando. Os sites devem usar apenas HTTPS e não fornecer alternativas de HTTP. Os usuários podem instalar plug-ins de navegador para impor sempre o uso de HTTPS nas solicitações.

Autenticação Baseada em Par de Chaves Públicas

Os ataques man-in-the-middle normalmente envolvem a falsificação de uma coisa ou outra. A autenticação baseada em par de chaves públicas, como RSA, pode ser usada em várias camadas da pilha para ajudar a garantir se as coisas com as quais você está se comunicando são realmente as coisas com as quais deseja se comunicar.

Abaixo está um exemplo do que pode acontecer quando o homem do meio se inserir.



O hacker está representando os dois lados da conversa para obter acesso aos fundos. Este exemplo vale para uma conversa com um cliente e um servidor, bem como conversas de pessoa para pessoa. No exemplo acima, o invasor intercepta uma chave pública e, com isso, pode transpor suas próprias credenciais para enganar as pessoas de cada lado, fazendo-as acreditar que estão se comunicando com segurança.